

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed March 11, 2005. Claims 1-22 were pending in the Application. In the Office Action, Claims 1-22 were rejected. In order to expedite prosecution of this Application, Applicants amend Claims 7, 14 and 19-22. Thus, Claims 1-22 remain pending in the Application. Applicants respectfully request reconsideration and favorable action in this case.

In the Office Action, the following actions were taken or matters were raised:

SPECIFICATION

The Examiner suggested that Applicants provide the serial numbers of related co-pending applications mentioned on page 1 of the specification. Applicants have so amended the indicated related applications portion of the specification to include such serial numbers. Favorable action is respectfully requested.

SECTION 112 REJECTIONS

Claims 12 and 13 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Specifically, the Examiner asserts that the term “binary pattern comparison” is a relative term which renders the claim indefinite. Applicants respectfully disagree.

Claim 12 recites “wherein comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the first signature and the first set of machine readable logic,” and Claim and 13 recites “wherein comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the second signature and the second set of machine readable logic.” Applicants respectfully refer the Examiner to page 16, line 26 to page 17, line 2, of Applicants’ specification which recites:

Each text-file 277A-277N may define a network-based exploit and comprise a logical description of an attack signature as well as IPS directives to execute upon an IPS evaluation of an intrusion-related event associated with the described attack signature. Each text file 277A-277N may be stored in a database 278A on storage media 276 and compiled by a compiler 280 into a respective machine-readable signature file 281A-281N that is stored in a database 278B. Each of the machine-readable signature files 281A-281N comprises binary logic representative of the attack signature as described in the respectively associated text-file 277A-277N.

(emphasis added). Further, page 21, lines 30 to page 22, line 20, of Applicants' specification recites:

As described hereinabove, an IPS application 91 of the present invention may perform signature matching on network frames by implementing a pattern matching algorithm, or other signature recognition technology. Preferably, signature files 281A-281N generated from compilation of text-files comprising text descriptions of attack signatures are passed to network filter service provider where a signature recognition technique is performed. . . Accordingly, the probe packet must pass through the network filter service provider 140 and the response generated thereby must pass therethrough as well. As the probe packet is passed to the protocol driver by the media access control driver 145, the network filter service provider may perform a signature analysis on the packet. Likewise, as the response packet generated by network stack 90 is passed to media access control driver 145, it first passes through network filter service provider 140 where a signature analysis may be made on it as well.

(emphasis added). Further, Applicants respectfully refer the Examiner to at least pages 23 and 24 of Applicants' specification which provides a detailed example of a signature analysis or comparison. Accordingly, Applicants submit that Claims 12 and 13, when read in light of Applicants' specification, reasonably apprise those skilled in the art both of the utilization and scope of the invention as defined thereby in compliance with 35 U.S.C. § 112, second paragraph. Thus, Applicants respectfully request that this rejection be withdrawn.

SECTION 102 REJECTIONS

Claims 19 and 20 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter “*Vaidya*”). Applicants respectfully traverse this rejection.

Of the rejected claims, Claim 19 is independent. Applicants respectfully submit that *Vaidya* does not disclose or even suggest each and every limitation of amended Claim 19. *Vaidya* appears to disclose comparison of a data packet with an attack signature profile for intrusion detection (*Vaidya*, abstract). However, *Vaidya* does not appear to disclose or even suggest “reading a response packet by the node, the response packet generated in response to reception of a first packet by the node,” “determining a signature of the response packet,” “comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature” and “determining the signature corresponds with the machine-readable logic” as recited by amended Claim 19 (emphasis added). Thus, for at least this reason, Applicants respectfully submit that *Vaidya* does not anticipate amended Claim 19.

Claim 20 that depends from independent Claim 19 is also not anticipated by *Vaidya* at least because it incorporates the limitations of Claim 19 and, also, adds additional elements that further distinguish *Vaidya*. Therefore, Applicants respectfully request that the rejection of Claim 20 be withdrawn.

SECTION 103 REJECTIONS

Claims 1-18, 21 and 22 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Vaidya* in view of U.S. Patent No. 6,578,147 issued to Shanklin et al. (hereinafter “*Shanklin*”). Applicants respectfully traverse this rejection.

Of the rejected claims, Claims 1, 7 and 14 are independent. Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests the limitations of independent Claims 1, 7 and 14. For example, independent

Claim 1 recites, at least in part, “reading a first packet received by the node,” “comparing [a] first signature [of the first packet] with a signature file comprising a first machine-readable logic representative of a first packet signature,” “determining the first signature corresponds with the first machine readable logic,” “reading a second packet generated by the node in response to reception of the first packet,” and “comparing [a] second signature [of the second packet] with the signature file” (emphasis added). Regarding independent Claims 1, 7 and 14, the Examiner admits that *Vaidya* does not explicitly disclose reading the response packet of the first packet (Office Action, page 4). However, the Examiner states that *Shanklin* teaches such limitation, and that it would have been obvious to modify *Vaidya* with the teaching of *Shanklin* for inspecting outgoing response packets (Office Action, page 4). Applicants respectfully disagree.

Shanklin appears to disclose a router 12 that inspects packets incoming from the external network to determine which should be forwarded into the local network 10, and that packets originating in the local network are inspected to determine whether they are to be forwarded to the external network (*Shanklin*, column 3, lines 30-34). However, neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests “reading a second packet generated by the node in response to reception of the first packet,” and “comparing [a] second signature [of the second packet] with the signature file” as recited by independent Claim 1. To the contrary, *Shanklin* does not appear to disclose or even suggest that the outgoing packets in *Shanklin* are in response to receipt of a first packet, not has the Examiner explicitly identified any such disclosure in *Shanklin*. Accordingly, for at least this reason, independent Claim 1 is patentable over the cited references.

Independent Claim 7, as amended, recites “reading a first packet,” “comparing [a] first signature [of the first packet] with a first instruction set comprising a first set of machine readable logic representative of a first packet signature,” “determining the first signature corresponds with the first set of machine readable logic,” “reading a second packet generated in response to reception of the first packet” and “comparing [a] second signature [of the second packet] with a second instruction set comprising a second set of machine readable logic representative of a second packet signature” (emphasis added), and independent Claim

14 recites a “network filter service provider operable to receive a first packet and . . . and compare [a] first signature [of the first packet] with a first instruction set comprising a first set of machine readable logic representative of a first packet signature and to determine a correspondence with the first set of machine readable logic” and “receive a second packet generated in response to receipt of the first packet and . . . compare [a] second signature [of the second packet] with a second instruction set comprising a second set of machine readable logic representative of a second packet signature and to determine a correspondence with the second set of machine readable logic” (emphasis added). Thus, at least for the reasons discussed above in connection with independent Claim 1, independent Claims 7 and 14 are patentable over the cited references.

Claims 2-6, 8-13 and 15-18 depend respectively from independent Claims 1, 7 and 14. Further, Claims 21 and 22 depend from independent Claim 19. For at least the reasons discussed above, independent Claims 1, 7, 14 and 19 are in condition for allowance. Therefore, Claims 2-6, 8-13, 15-18, 21 and 22 are also in condition for allowance. Accordingly, Applicants respectfully request that the rejection of Claims 1-18, 21 and 22 be withdrawn.

CONCLUSION

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicant has overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By: 
James L. Baudino
Reg. No. 43,486

Date: June 10, 2005

Correspondence to:
L.Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
Tel. 970-898-3884